United States District Court
District of Massachusetts

United States of America,	)	
v.	)	
Robert Daigle,	)	**Criminal Action No. 22-10035-NMG**
Defendant.	)	

MEMORANDUM & ORDER

GORTON, J.

Defendant Robert Daigle ("Daigle" or "defendant") has been indicted on one count of receipt of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1). The government also brings a child pornography forfeiture allegation under 18 U.S.C. § 2253.

Currently before the Court is defendant's motion to suppress evidence (Docket No. 86). For the reasons that follow, that motion will be denied.

I. Background

A. Background on Freenet

The motion largely concerns the mechanics of the peer-to-peer file sharing network known as "Freenet." According to the affidavit, when a user uploads a file to Freenet, it is divided into so-called "blocks" each of which is encrypted and

distributed across the Freenet network. Users each provide space on their hard drives to store those blocks.

Freenet users are unable to conduct keyword searches for Freenet files but rather can only download a file by obtaining a "key". Keys can be obtained through several means including from online message boards or directly from other users.

Once a user clicks or inputs a key, the download process for a file begins. By virtue of the divide and distribute model described above, completing a download with a key requires that a Freenet user request pieces of the file from other users (known as "peers"). Not every peer, however, has the requested blocks. Thus, if a peer does not have the block, that peer will divide the request and ask a number of its own peers for the missing blocks.

The process of requesting blocks can continue up to 18 levels. The affidavit states that if the 1level limit is reached, a "signal is returned to the user's computer and the request is sent to another of the user's peers." Defendant contends that the characterization in the affidavit is misleading because it fails to clarify that a request can hit the 18-level limit without the requested piece being found (and thus, the blocks are unassembled and the file unretrieved).

Defendant emphasizes that the peer-to-peer process of obtaining the blocks that compose a file results in anonymity

and, therefore, it is difficult to ascertain if a peer is the original requester of a block or a "relayer" of the request.

According to the affidavit, since about 2011, law enforcement officers have investigated the trafficking of child pornography on Freenet by collecting keys associated with suspected child pornography files. Those files are referred to as "files of interest." Defendant contends that the database of files of interest is over-inclusive because, even where a key is found on an "on-topic" message board, the contents of a file are unknown to users until the blocks are reassembled.

B. The Investigation

In January, 2022, Federal Bureau of Investigation ("FBI") Agents executed a search warrant ("the Warrant") at defendant's residence at 270 Florence Road in Waltham, Massachusetts and conducted an interview of defendant. The Warrant was supported by an affidavit of FBI Special Agent Brian O'Sullivan ("O'Sullivan").

The affidavit avers that on two consecutive days in April, 2021, a Freenet user with IP address 96.230.244.94 requested pieces of three files containing child pornography from a law enforcement Freenet computer. Using public search tools and administrative subpoenas, investigators determined that the IP address is associated with a Verizon account registered at defendant's home to "Gerard Daigle." Law enforcement obtained

the keys for each of the files containing child pornography between 2011 and the present. Investigators had not determined, however, how defendant obtained those keys. The affidavit also contained detailed descriptions of the operation of Freenet and the characteristics common to consumers of child pornography.

II. Motion to Suppress

Defendant contends that 1) there was insufficient probable cause to support the Warrant authorizing a search of his residence and 2) the Court should hold a Franks hearing in light of purported misrepresentations in the affidavit.

A. Probable Cause

The finding of a magistrate judge as to probable cause is entitled to "great deference". Illinois v. Gates, 462 U.S. 213, 236 (1983). Reversal of such a finding is appropriate only if there is "no substantial basis for concluding that probable cause existed." United States v. Dixon, 787 F.3d 55, 58-59 (1st Cir. 2015) (citation omitted).

Probable cause exists when, based upon common sense and the totality of the circumstances, "there is a fair probability that contraband or evidence of a crime will be found in a particular place." Gates, 462 U.S. at 238. A warrant application must contain facts demonstrating probable cause to believe that (1) a crime has been committed (the "commission" element) and (2)

enumerated evidence of the offense will be found at the place searched (the "nexus" element). United States v. Feliz, 182 F.3d 82, 86 (1st Cir. 1999).

Defendant contends that the Warrant lacks probable cause because the affidavit describes no evidence: 1) demonstrating that defendant possessed files containing child pornography, 2) that defendant intended to request files containing child pornography or 3) that is not stale.

As defendant confirms, Freenet's divide-and-distribute model enables investigators to determine if users request pieces of "files of interest" known to contain child pornography. Defendant insists that the affidavit fails to establish whether he was ultimately successful in downloading, and thus obtaining, the files containing child pornography. He also asserts that the affidavit fails to describe evidence that he intended to access child pornography because investigators did not determine how the keys to the files of interest were obtained.

Defendant's contentions are unavailing. A finding of probable cause requires only "a fair probability on which reasonable and prudent [people,] not legal technicians, act." Florida v. Harris, 568 U.S. 237, 244 (2013) (quoting Gates, 462 U.S. at 238). Here, the facts gathered and surrounding circumstances enabled investigators reasonably to infer that

evidence related to child pornography would be found at defendant's residence.

The affidavit avers that, within a short period of time, a user with an IP address associated with defendant's residence requested pieces of three different files all known to law enforcement to contain child pornography. Based on the affiant's assessment of, inter alia, the number of requested blocks, the total number of blocks needed to assemble the file and the number of peers of the user, investigators reasonably inferred that the user was the original requestor of those files. Those facts alone support a substantial likelihood that a user at defendant's residence intentionally requested the files to gain access to child pornography.

It is true that investigators did not ascertain how the user initially accessed the keys to those files or whether the downloads were completed. Nonetheless, it was reasonable for investigators to infer that three separate requests for three different files known to contain child pornography within a short timeframe is beyond mere coincidence. Rather, those facts suggest that the user intended to access the files for the purposes of obtaining child pornography. Furthermore, the anonymized nature of Freenet, while independently insufficient to establish probable cause, enhances the probability that a user at defendant's residence sought child pornography and not

some other innocuous material. See United States v. Anzalone, 923 F.3d 1, 5 (1st Cir. 2019).

Finally, defendant asserts that the evidence was stale because the Freenet blocks had been requested eight months before investigators applied for the Warrant. He relies largely on the Second Circuit decision in United States v. Raymonda, 780 F.3d 105 (2d Cir. 2015), where that Court held that there was insufficient probable cause to support a warrant based on nine-month-old evidence that a web user at defendant's address

> opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files.

Id. at 117. The Court did not, however, deem the evidence excessively stale because it was nine months old. Rather, the Court held that given the age of the evidence, more corroborating circumstances demonstrating that defendant had intended to collect child pornography was needed. Id. Such corroboration was lacking because 1) there was no evidence that the subject website was sought out for the purpose of discovering child pornography, 2) investigators only discovered the website through an innocuous link on another site not associated with child pornography and 3) there was no evidence defendant saved or even viewed all of the images.

The circumstances here provide a stronger foundation linking defendant to the illicit procurement of child pornography. The affidavit avers that a user with an IP address associated with defendant's residence requested blocks of files known to authorities to contain child pornography three times within a short span of time. Authorities were able to establish with sufficient likelihood based on

> the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had

that the user was an original requestor of the files to be downloaded and not simply relaying the request.

By contrast, the affidavit in Raymonda did not establish that the site was known to authorities a priori to contain child pornography or that defendant had even viewed most of the images that were readily accessible on the website. Thus, the information in the affidavit was at least as likely to reflect

> an innocent user inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window.

Id. Unlike in Raymonda, the facts here sufficiently manifest an intention to access illicit images.

B. Franks Hearing

Defendant also requests a Franks hearing and purports that the affidavit contains several omissions and misstatements. For a defendant to be entitled to a Franks hearing, he must make a preliminary showing that 1) a false statement knowingly and intentionally, or with reckless disregard for the truth, was included in the affidavit, and 2) the alleged misrepresentation was necessary to establish probable cause. Franks v. Delaware, 438 U.S. 154, 155-56 (1978). To justify a hearing, defendant must make a sufficient showing as to both elements. See United States v. Rigaud, 684 F.3d 169, 173 (1st Cir. 2012).

Defendant takes issue with three statements and purported omissions in the affidavit: 1) the omission of the possibility that a Freenet request could fail and that the file would not be returned 2) the claim that the user requested blocks over the course of multiple days and 3) the statement that the user requested blocks associated with files known to contain child pornography "which would have required him to ascertain the specific keys associated with those files."

The Court finds that the statements and purported omission are not materially misleading and do not warrant holding a Franks hearing. First, the affidavit is abundantly clear that when a Freenet user requests blocks of a file to complete a download the request

> does not indicate whether-or-not the user successfully retrieved all of the necessary pieces to successfully download the file.

That statement adequately explains that a request may fail by raising the possibility that retrieval of all blocks was not completed.

Nor is the averment that the user requested blocks over multiple days materially misleading. The government has adduced evidence that blocks were requested on April 11 and 12, 2021, whereas defendant suggests that the requests were initiated all within a 10-minute timeframe. Both versions of events can be true because requests take time to be completed. Whether the request occurred in a 10-minute timeframe or over the course of two days has no bearing on the probable cause determination. Of greater consequence is that there were three separate requests all within a relatively short period of time.

Finally, the Court finds that the statement that the user requested blocks associated with files known to contain child pornography "which would have required him to ascertain the specific keys associated with those files" is not misleading. Defendant asserts that the statement implies that he intended to access child pornography before he found the keys to the three files of interest. That may be true but, nonetheless, the affidavit adequately establishes intent by describing corroborating circumstances. Accordingly, the implication that

defendant sought the keys with the intention of accessing child pornography is not misleading. Averments in the affidavit that investigators did not determine how defendant found the keys also tempers the inference.

C. Good Faith Exception

Even were this Court to conclude that the finding of the magistrate judge of probable cause was deficient, the search easily falls within the parameters of the "good faith" exception to the exclusionary rule. See United States v. Leon, 468 U.S. 897, 922 (1984) (holding that objectively reasonable reliance on a subsequently invalidated search warrant does not justify invoking the exclusionary rule). Under that rule, suppression is warranted if the affiant 1) recklessly or deliberately misled the magistrate judge, 2) the magistrate judge completely abandoned her judicial role in issuing the warrant, 3) the warrant was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" or 4) the warrant was facially deficient. Id. at 923.

None of those circumstances is present here. As discussed supra, defendant has uncovered no material misstatements in the affidavit. Nor is the probable cause determination so lacking as to put investigators on notice of its deficiencies. Rather, as discussed above, the probable cause determination reflects

the fair probability that investigators would find evidence of child pornography at defendant's residence.

ORDER

For the foregoing reasons, the motion of defendant, Robert Daigle, to suppress evidence and to hold a Franks hearing (Docket No. 86) is **DENIED**.

So ordered.

/s/ Nathaniel M. Gorton
Nathaniel M. Gorton
United States District Judge

Dated: April 24, 2024